FRAUD ALERT

Educating South Carolina's Consumers

A Publication of the South Carolina Task Force on Fraud

September 14, 2005 **Volume 1, Issue 3** **www.scconsumer.gov**

If you would like to receive a free subscription to the *Fraud Alert*,
contact the South Carolina Department of Consumer Affairs at 803.734.4200 or e-mail Fraud_Alert@dca.state.sc.us

Thinking of the Victims of Hurricane Katrina: Here's How to Help

A Guide to Giving Wisely

In response to the devastation of Hurricane Katrina, many South Carolinians are searching for ways to help the victims. The SC Department of Consumer Affairs advises that the best way to help immediately is to donate money directly to established national relief organizations. Here are a few tips to help consumers:

- Donate to recognized charities you have given to before. Watch out for charities that have sprung up overnight. They may be well-meaning, but lack the infrastructure to provide assistance. And be wary of charities with names that sound like familiar or nationally known organizations. Some phony charities use names that sound or look like those of respected, legitimate organizations.
- Give directly to the charity, not the solicitors for the charity. Solicitors take a portion of the proceeds to cover their costs, which leaves less for victim assistance.
- Do not provide personal or financial information – including your Social Security number or credit card and bank account numbers – to anyone who solicits from you. Scam artists can use this information to commit fraud.
- Check out any charities before you donate. The Secretary of State has a list of all official charities.
- Do not give or send cash. For security and tax record purposes, contribute by check or credit card. Write the official name of the charity on your check.

If you are approached in person ask for identification. Many states require paid fundraisers to identify themselves as such and to name the charity for which they are soliciting.

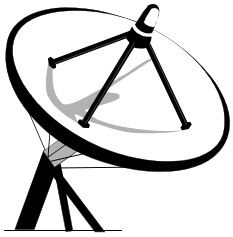
Hurricane Katrina Victims are at Risk for ID Theft

Here is how you can protect your data during a catastophic event:

- If you are faced with an evacuation order or some other circumstance that forces you to vacate your home, protect the premises with the strongest possible security measures.
- Shred, burn, or otherwise destroy any unneeded documents containing personal information, such as Social Security and driver's license numbers, credit card and bank account numbers, phone numbers, and postal and email addresses.
- If identity theft is prevalent in your area, consider leasing a safe deposit box at a local bank in which to secure personal documents.
- Any items containing personal identifiers that are not destroyed or safely secured should be in your possession at all times. This, in fact, is one of the rare instances in which an individual should carry a Social Security card, birth certificate, passport, and similar articles.

How Identity Thieves Use Your Personal Information

- They may call your credit card issuer to change the billing address on your credit card account. The imposter then runs up charges on your account. Because your bills are being sent to a different address, it may be some time before you realize there's a problem.
- They may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.
- They may establish phone or wireless service in your name.
- They may open a bank account in your name and write bad checks on that account.
- They may counterfeit checks,credit or debit cards or authorize electronic transfers in your name, and drain your bank account.
- They may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- They may buy a car by taking out an auto loan in your name.
- They may get identification such as a driver's license issued with their picture, in your name.
- They may get a job or file fraudulent tax returns in your name.
- They may give your name to the police during an arrest.



Wardrivers Could Be In Your Area

Everyone knows advances in technology have been great over the past decade. But such great advances has also produced many problems. Not too long ago computers were heavy pieces of equipment that were very expensive, and required a staff of a dozen to operate it, with no communication components. Today's computers are cheap, portable, somewhat simple and connected to the outside world. With the introduction of an interconnection systems, came illegal and immoral activities. Computer criminals today, who are sometimes called hackers, are now able to tap into your Internet connection, personal computer, or your personal information with a click of the keyboard.

The latest craze in the hacking world is called Wardriving. Wardriving is an activity consisting of driving around with a Wi-Fi equipped laptop or a PDA in a vehicle and detecting Wi-Fi wireless networks. Wardivers cruise with laptops, inexpensive antennas and software that can detect the existence of a wireless network within about 300 feet and pinpoint its location using a global positioning device. With the right equipment hackers then access your wireless computer system, without the user even knowing it, and access personal information from your computer.

To protect yourself from being a victim of wardriving, first make sure you set your router to the Wired Equivalent Privacy (WEP), a security protocol for wireless local area networks. Also make sure your firewall is turned on. Experts say that having your equipment secured from wardriving will cost you a couple hundred dollars, but the price is well worth it.

Special Alert
Red Cross Scam

Some people are taking advantage of the disaster that Katrina has left in her path. Multi-state distribution of "phishing" emails has gone out impersonating the Red Cross. Links embodied within the email will take you to a fake Red Cross site. It's wise to disregard any email solicitations for donations from the Red Cross or other organizations. Go to the Red Cross website personally to make your donations. For information on hurricane preparedness request a copy of our Hurricane Preparedness newsletter by contacting the SCDCA at 803-734-4200 or (800) 922-1594 (toll free in SC). Also visit our Website at **www.scconsumer.gov.**

It's a Scam!
Be On the Lookout

The Valued Customer Scam:

This scam involves consumers receiving phone calls claiming to be from a major retailer or wholesaler in town. The caller informs the consumer that they are recipients of a $500.00 shopping voucher for being a "valued customer." In order to receive the vouchers, however, consumers are asked for their bank account information so that a small shipping charge can automatically be withdrawn from their checking account. Consumers who provided this information found that their accounts had one or more unauthorized transactions, many from unfamiliar companies. In at least one case the consumer's entire account was withdrawn, causing overdraft problems and large bank fees.

Two-Week Degrees:

Consumers should be suspicious of companies offering Bachelors, Masters', MBA's, Doctorate & Ph.D. degrees within two weeks. Consumers are said to receive these degrees based on their present knowledge and life experiences. In order for the consumer to receive credit for the degree, they must first supply their credit card and personal banking information. The degrees require no testing, classes, books or examinations.

Special Society Scam:

The department received reports from consumers regarding a letter they received from a "secret society". The letter claims that by completing the attached form, which requests personal information, the victim will become a member of this "secret society". The "secret society" claims that after becoming a member, you will supposedly "gain great wealth and success."

Tips to Avoid Hurricane Relief Scams

- Be suspicious of anyone wanting on-the-spot donations or refusing to provide written, verifiable information about the organization.
- Don't assume a charity is legitimate based on the name.
- Use a credit card or check for donating, rather than cash, so you'll have record of the expense.
- Be wary of organizations that offer to send a "runner" to pick up your donation. Reputable charities are willing to wait for your contribution.
- Consumer have the right to ask for an organization's financial report and its federal tax identification number.
- Remember that organizations like the Red Cross will never call you and ask you to make a donation.

If you have been a victim of a scam or want more information about these and other scams, contact the South Carolina Department of Consumer Affairs (803) 734-4200 or (800) 922-1594 (toll free in SC). You can also visit our Website at www.scconsumer.gov.

South Carolina Department of Consumer Affairs	*Office of the Attorney General*	*South Carolina Law Enforcement Division*	*South Carolina Sheriffs' Association*	*Federal Bureau of Investigation*	*United States Attorney's Office*	*United States Secret Service*	*South Carolina Police Chiefs' Association*
3600 Forest Drive Suite 300 P.O. Box 5757 Columbia, SC 29250 www.scconsumer.gov 1.800.922.1594 (803)734.4200	1000 Assembly Street Suite 519 P.O. Box 11549 Columbia, SC 29211 www.scattorneygeneral.org (803)734.3970	4400 Broad River Road P.O.Box 21398 Columbia, SC 29221 www.sled.state.sc.us (803)737.9000	112 West Park Blvd. P.O.Box 21428 Columbia, SC 29210 www.sheriffsc.com (803)772.1101	151 Westpark Blvd. Columbia, SC 29210 www.fbi.gov (803)551.4200	1441 Main Street Suite 500 Columbia, SC 29201 www.usdoj.gov/usao/sc/ (803)929.3000	107 Westpark Blvd. Suite 301 Columbia, SC 29210 www.secretservice.gov (803)772.4015	4701 Arcadia Road P.O.Box61170 Columbia, SC 29260 www.scpca.org (803)790.5042